



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/874,795	06/05/2001	Geoffrey R. Hird	028410-0016	5815
20350 7590 01/31/2007 TOWNSEND AND TOWNSEND AND CREW, LLP TWO EMBARCADERO CENTER EIGHTH FLOOR SAN FRANCISCO, CA 94111-3834			EXAMINER KLIMACH, PAULA W	
			ART UNIT 2135	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE 3 MONTHS			MAIL DATE 01/31/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/874,795	HIRD, GEOFFREY R.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 November 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,4-20,23-31 and 34-43 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,4-20,23-31 and 34-43 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>11/14/06</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 11/14/06. The amendment filed on 11/14/06 have been entered and made of record. Therefore, presently pending claims are 1, 4-20, 23-31, and 34-43.

Response to Arguments

Applicant's arguments filed 11/14/06 have been fully considered, however the Zingher reference teaches the limitations that the applicant argues are not recited by Pavlov and Spratte.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 4-20, 23-31, and 34-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pavlov (4,614,861) in view of Spratte (5,764,766) and further in view of Zingher et al (5,731,575).

In reference to claims 1, 20, 31, 42-43, Pavlov discloses a system a self-contained card that has the ability to verify a personal identification number that is entered directly into the body by way of a keyboard (abstract). The self-contained card comprises: (a) a computer-implemented input for receiving a input access code (Fig_1 part 12 in combination with column

Art Unit: 2135

11 lines 60-67); output said datum reproducing said at least a portion of said user's confidential datum (TIC) if said input access code equals said user's access code (column 12 lines 15-30); and (d) said generation of said output datum occurring without dependence on any storage of any form of said at least a portion of said confidential datum (column 12 lines 29-67).

Although Pavlov discloses the generation of confidential data, TIC, Pavlov does not disclose a seed derivation module operatively connected to said input, for deriving a seed usable to generate at least a portion of said confidential datum; a seed-based data generation module implementing a predetermined data generation protocol that was previously used by a seed-based initialization of said confidential datum of said user, containing a representation of a seed-access code relationship, and configured to generate an output datum by digitally processing said derived seed in accordance with said seed-access code relationship.

Spratte discloses a system and method for encrypting data communication comprising the generation of an encryption key (abstract). The applicant does not define a data generation protocol; as a result, a data generation protocol is a method of generating data. In addition, the applicant does not define a seed access code. A value generated using the access code or identification number. The system of Spratte includes a seed derivation module operatively connected to said input, for deriving a seed usable to generate at least a portion of said confidential datum (column 2 line 65 to column 3 line 1); a seed-based data generation module implementing a predetermined data generation protocol that was previously used by a seed-based initialization of said confidential datum of said user, containing a representation of a seed-access code relationship, and configured to generate an output datum (encryption key) by digitally

Art Unit: 2135

processing (hashed) said derived seed in accordance with said seed-access code relationship (column 3 lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system of Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

Pavlov and Spratte do not expressly disclose a system wherein for at least one input access code not equaling said user's access code, said output datum has the characteristic appearance of said at least a portion of said confidential datum, but said output datum does not reproduce at least a portion of said user's confidential datum.

Although Pavlov discloses checking the matching of the access code, Pavlov does not expressly disclose the seed based data generation module generates an invalid output datum having the appearance of the user's confidential datum

Zingher discloses a system wherein when the access code does not match then the module generates a message that the request exceeds the maximum allowable withdrawal at this machine (column 9 lines 9-23). By generating the message, the system of Zinger, generates an invalid output datum having the appearance of the user's confidential datum. The datum is invalid because, as stated by the system of Zingher, (column 9 lines 14-16) the maximum is actually a value of \$500 or \$300. However the output datum has the appearance of the user's confidential datum since the system does not provide the actual amount that is available and there appears like the confidential datum, but is invalid.

Art Unit: 2135

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to the generation of an output datum as a function of the input access code as in Zingher in the system of Pavlov. One of ordinary skill in the art would have been motivated to do this because in the case where the confidential data is the user's account information and the user is in a distressed situation, providing the information may prevent the robber does not become agitated and harm the victim (Zingher column 9 lines 5-8).

In reference to claims 4, 23, and 34, Pavlov discloses a system where said access code is a PIN (Fig_7).

Spratte discloses a system and method for encrypting data communication comprising the generation of an encryption key (abstract); and said confidential datum includes an asymmetric cryptographic key (column 3 lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system of Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claim 5, Pavlov does not discloses a system where said output datum has the characteristic appearance of an asymmetric cryptographic key.

Spratte discloses a system and method for encrypting data communication comprising the generation of an encryption key (abstract); said output datum has the characteristic appearance of an asymmetric cryptographic key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system fo Pavlov. One of ordinary skill in

the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claim 6, Pavlov discloses a system wherein the access code is a PIN (Fig_7).

Spratte discloses a system and method for encrypting data communication comprising the generation of an encryption key (abstract); and said confidential datum includes a symmetric cryptographic key (column 3 lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system fo Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claims 7, 24, 35, and 36, where said seed-access code relationship is a identity relationship, so that said derived seed equals said input access code (Fig_7).

In reference to claims 8 and 25, a system where said seed-access code relationship represents said derived seed as a padded version of said input access code.

Spratte discloses a system and method for encrypting data communication comprising the generation of an encryption key (abstract); and where said seed-access code relationship represents said derived seed as a padded version of said input access code. (column 3 lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system of Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claims 9, 26, and 37, Pavlov does not disclose a system where said seed-access code relationship includes a version of said initial seed masked by user's access code.

Spratte discloses a system and method for encrypting data communication comprising the generation of an encryption key (abstract); and where said seed-access code relationship includes a version of said initial seed masked by user's access code (column 3 lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system fo Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claims 10, 27, and 38, where: (i) said masked version of said initial seed includes an XOR of said initial seed with said user's access code; and (ii) said processing of said derived seed in accordance with said seed-access code relationship includes XORing said masked version of said initial seed with said derived seed.

Spratte discloses a system wherein the initial seed (salt) is combined with the user's access code (primary key). XOR is a form of combining initial seed with the user's access code. The processing of the derived seed (hashing) as disclosed by Spratte only discloses Message Digest 5 as an example; therefore XORing is one another possible way to implement a hash function.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system fo Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claim 11, Pavlov does not disclose a system further comprising program code for updating a user's old access code with a user's new access code by replacing said stored masked version of said initial seed with its value XORed with said user's old access code XORed with id user's new access code.

Spratte discloses a system further comprising program code for updating a user's old access code with a user's new access code by replacing said stored masked version of said initial seed with its value XORed with said user's old access code XORed with id user's new access code (column 3 lines 29-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system of Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claims 12, 28, and 39, Pavlov does not disclose a system where: (i) said seed-access code relationship includes a truncated version of said initial seed capable of being concatenated with said input access code to form said derived seed; and (ii) said processing of said derived seed in accordance with said seed-access code relationship includes concatenating said truncated version of said initial seed with said input access code.

Spatte discloses combining the salt with the primary key which results in the said seed-access code relationship includes a truncated version of said initial seed capable of being concatenated with said input access code to form said derived seed. The hash result in the concatenation and truncation of the encryption key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system fo Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claims 13, 29, and 40, Pavlov does not disclose a system where: (i) said seed-access code relationship includes values of, and associations between, a plurality of possible values of said input access code and a corresponding plurality of possible values of said derived seed; and (ii) said processing of said derived seed in accordance with said seed-access code relationship includes looking up and outputting said possible value of said derived seed corresponding to said input access code.

Spatte discloses a system where (i) said seed-access code relationship includes values of, and associations between, a plurality of possible values of said input access code and a corresponding plurality of possible values of said derived seed; and (ii) said processing of said derived seed in accordance with said seed-access code relationship includes looking up and outputting said possible value of said derived seed corresponding to said input access code (column 3 lines 30-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system fo Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claims 14, 30, and 41, Pavlov does not disclose a system where: (1) said seed derivation module is merged with said data generation module; (2) said output datum includes said derived seed.

Spatte discloses a system where: (1) said seed derivation module is merged with said data generation module; (2) said output datum includes said derived seed (column 3 lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system of Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claim 15, where said confidential datum includes a private key of said user, and said output datum has the characteristic appearance of a private key.

Spatte discloses a system where: said confidential datum includes a private key of said user, and said output datum has the characteristic appearance of a private key (column 3 lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system of Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claim 16, where said user's public key corresponding to said user's private key is pseudo-public.

Spatte discloses a system where: said user's public key corresponding to said user's private key is pseudo-public (column 3 lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system fo Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claim 17, a system further comprising a digital certificate containing said pseudo-public key.

Spatte discloses a system further comprising a digital certificate containing said pseudo-public key (column 3 lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system fo Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claim 18 where said digital certificate includes an encrypted version of said user's pseudo-public key encrypted under a certifier's key which is not verifiable except by authorized verifiers.

Spatte discloses a system with an encryption key (column 3 lines 1-10). The digital certificate is a form of security that contains the key and certifies the ownership of the key and therefore added security.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate a key as in Spratte in the system fo Pavlov. One of ordinary skill in the art would have been motivated to do this because it would create keys that meet export conditions, but are unique enough to make them difficult to hack.

In reference to claim 19, Pavlov discloses a system that is configured to be remotely accessible to a roaming user across a network (column 9 lines 64-66).


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Friday, January 26, 2007


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100